ATTACHMENT B

DECLARATION OF JOSEPH LUM

UNDER 37 CFR §1.132

I, Joey Philip Lum, hereby declare as follows:

1. My residence address is 2 Malaga, Irvine, CA 92614.

2. I hold a BSEE degree, obtained from UCLA, and an MSEE degree, obtained from Loyola Marymount University.

3. Since April 2001 I have been employed by Sharp Laboratories of America, Inc. ("SLA"), 5901 Bolsa Blvd, Huntington Beach, CA 92647. My title at SLA is Senior Engineer. My responsibilities include embedded firmware development for MFPs; implementing security, LDAP, and networking functions.

4. I have read the claims for the patent application in question, System and Method for Secure Communications with Network Printers, invented by Sridhar Dathathraya, Serial Number 09/944,695 (the Applicant). I have read the relevant parts of the Office Action dated June 27, 2005, where claims 1-8, 10-25, and 27-35 have been rejected as obvious over US 6,862,583, Mazzagatte, in view of US 6,385,728, DeBry. In summary, it is my opinion that the cited references do not make obvious the Applicant's claims.

5. Generally, Mazzagatte describes a system where the printer accepts an unencrypted document sent using a secure protocol. As a

protection mechanism, the printer stores the document in an encrypted format, where a symmetric (secret) key is used to encrypt the document, and the printer's asymmetric (public) key is used to encrypt the secret key. Before the document can be printed, the printer's private key is used to recover the secret key, which can then be used to decrypt the document. The Office Action, in the first two lines of page 4, states that Mazzagatte does not describe the encryption of data using a public key. In my reading of Mazzagatte, I can only find one brief mention of a process, at column 8, lines 5-18, where the print driver encrypts the document prior to transmission, so that it can be sent to a printer using a non-secure protocol.

5. DeBry describes a system that permits a client to transfer a document from a file source, to a printer, without the client ever obtaining a copy of the document. A significant portion of the patent is devoted to the description of a "will-call certificate". DeBry only provides one example of how his process can be used to print a document at a printer, at column 10, line 28, through column 11, line 15. DeBry encrypts a document with a secret (symmetric) key, and then encrypts the secret key with the recipient's public key. At the target printer, the printer uses its private key to recover the secret key. Once the secret key is recovered, the document can be decrypted. This is exactly the same process that DeBry describes in his Background Section (column 2, lines 54 through 63), as a hybrid (digital envelop) process that has greater security than a pure secret key process, but greater speed (less computation) than a pure asymmetric (public/private) key process.

6. I have read the Applicant's response accompanying this affidavit, and I concur with its reasoning. In my opinion, the combination of Mazzagatte and DeBry do not make the inventions of claims 1, 12, 19, and 29

obvious. More specifically, I have been asked to consider whether DeBry suggests a modification to Mazzagatte that would make the claimed inventions obvious. I see no comments or drawings in the DeBry patent that would suggest to me, or any other skilled artisan, that the Mazzagatte's document delivery process can be modified in such a way as to suggest the Applicant's claims. That is, I do not see how DeBry's digital envelop process can be adapted for use in Mazzagatte's system. The will-call certificate is a key element of security in DeBry's system. However, there is no means for Mazzagatte to enable a will-call certificate. Without the will-call certificate, Mazzagatte's system cannot use the digital envelop described by DeBry for the transportation of a document to a printer from a print driver.

Even more important however, even if key elements from DeBry could logically be adapted for use in Mazzagatte's system, the result would not describe the Applicant's claims. Both DeBry and Mazzagatte describe the use of asymmetric keys, but neither reference describes a process where the user controls the private key. Mazzagatte seeks to protect documents stored in the server. To that end, the printer accessing the server controls the private key. DeBry seeks to protect a file source. To that end, the file source controls the private key. However, the focus of the Applicant's invention is different. The Applicant is seeking to protect the person who is printing a document. To that end, the person printing controls the private key. Since the user does not control the private key, neither of the prior art processes is as secure as the Applicant's claimed process, as least from the point of view of the user.

7. In summary, the combination of the Mazzagatte and DeBry do not make the inventions of claims 1-8, 10-25, and 27-35 obvious, since they do not suggest that a user can best protect their documents by

controlling their own private key. Mazzagatte's printer uses a private key to protect files that are kept in storage before printing, and DeBry uses a private key to protect a file that is accessed, but not owned, by a user. The claimed invention primarily protects a user who is sending a document to a printer for printing. I believe that an expert would not think the claimed invention obvious in light of the prior art, since the focus of protection is different. In fact, the prior art can be said to protect a system *from* a user.

8. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful, false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United State Code and that such willful, false statements may jeopardize the validity of the application or any patent issuing thereon.

8-10-05
Date

Joey Lum
Joey Lum